Représentant les avocats d'Europe
Representing Europe's lawyers

RECOMMANDATION DU CCBE SUR LA MISE EN OEUVRE DE LA DIRECTIVE SUR LA RETENTION DE DONNEES

Conseil des barreaux européens – Council of Bars and Law Societies of Europe
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.org – www.ccbe.org

RECOMMANDATION DU CCBE SUR LA DIRECTIVE SUR LA DETENTION DE DONNEES

Dans le présent document, le CCBE publie ses recommandations aux barreaux membres relatives à la mise en œuvre de la directive sur la rétention de données (Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE).

Au cours du processus législatif, le CCBE a fait part de ses vives inquiétudes quant à un certain nombre de points mentionnés ci-dessous. Cette directive est entrée en vigueur le 3 mai 2006 et devra être transposée en droit national avant le 15 septembre 2007 avec la possibilité de retarder l'application jusqu'au 15 mars 2009 pour les données de trafic Internet.

Le CCBE invite ses membres à appeler leurs législateurs nationaux à répondre aux craintes de la profession d'avocat lors de la transposition de la directive sur la rétention de données. A cette fin, le CCBE a rédigé une recommandation qui pourrait aider ses membres dans cette tâche.

Introduction

Le CCBE soutient la lutte contre le terrorisme et la criminalité. Toutefois, il est inquiet de voir le nombre d'initiatives croissantes prises au niveau européen qui, sous le couvert de la lutte contre le terrorisme, violent gravement les droits et libertés fondamentales.

L'objectif de la directive sur la détention de données est d'harmoniser les lois des Etats membres en matière de rétention de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications. Elle oblige les Etats membres à disposer d'un cadre juridique établissant la rétention de données de trafic et de données de localisation pour une durée allant de minimum six mois à maximum deux ans. Les informations obtenues par les données de trafic et de localisation constituent des questions importantes, d'où l'intérêt d'une telle législation pour les gouvernements. Le fait de pouvoir voir quand, où, comment et combien de fois telle personne consulte un avocat remet sérieusement en cause la confidentialité des relations du client avec son avocat et l'exercice même des droits de la défense.

Le CCBE s'est opposé à la directive sur la rétention de données qui, d'une part, viole le secret professionnel car elle ne fait pas de différence entre les différentes données et, d'autre part, comprend un certain nombre de failles et d'incertitudes (voir ci-dessous pour des informations complémentaires). Le CCBE a émis deux réserves spécifiques : (1) le secret professionnel n'est pas garanti lorsque les gouvernements auront accès aux données retenues et (2) une autorisation judiciaire préalable n'est pas nécessaire pour que le gouvernement accède aux données.

En soutien de l'avis du CCBE sur le secret professionnel, le Parlement européen a adopté une résolution législative en même temps qu'il a adopté la directive sur la rétention de données. La partie de la résolution du 14 décembre 2005 (P6_TA (2005)0512, A6-0365/2005) souligne la nécessité de garantir le secret professionnel :

« Le Parlement européen (…) 4. considère que les États membres ont le droit d'appliquer leurs principes constitutionnels nationaux et estime notamment que le ***secret professionnel*** *sera également respecté dans le cadre de l'application de la présente directive ; »*

Quant à l'autorisation judiciaire préalable, la note d'information ci-dessous établit de manière plus détaillée le caractère vague et les dysfonctionnements de la directive qui rendent l'autorisation judiciaire préalable impérative pour la protection des droits des citoyens.

En conséquence, le CCBE appelle ses membres à préserver en particulier le secret professionnel et l'autorisation judiciaire préalable lors de la transposition par le législateur national de la directive sur la rétention de données en droit national.

Recommandations

Le CCBE appelle ses membres à inviter leurs législateurs nationaux à veiller :

1. **à garantir le secret professionnel de l'avocat lors de l'accès aux données de trafic et de communication ayant fait l'objet de rétention par les gouvernements et autres autorités compétentes ;**

2. **à accorder l'accès uniquement après une autorisation judiciaire ;**

3. **à ce qu'après l'accès aux données par le gouvernement et les autorités policières et judiciaires, elles soient uniquement utilisées et conservées tant que cela se révèle nécessaire à l'objectif pour lequel elles ont été originellement fournies telles que protégées par l'article 6 de la directive 95/46/CE[1] et l'article 6, paragraphe 1 de la directive 2002/58/CE[2] ;**

4. **à garantir un niveau élevé de mesures de protection qui préservent le principe de respect de la vie privée et de la confidentialité des communications protégées en vertu des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne et de l'article 8 de la Convention européenne des droits de l'homme.**

Contexte

Il convient de noter que jusqu'à présent, le droit communautaire visait à protéger les personnes physiques à l'égard du traitement des données à caractère personnel (directive 95/46/CE). Cette directive interdisait la conservation de communications et de données de trafic par des personnes autres que les utilisateurs ou établissait au moins comme condition préliminaire l'obligation de rendre les données anonymes (directives 95/46/CE et 2002/58/CE) lors de leur conservation pour une durée limitée, notamment à des fins de facturation. Conformément à la directive 2002/58/CE, la rétention de données reste en tout cas une exception et se limite strictement aux dispositions de l'article 15 de la directive 2002/58/CE[3].

---

[1] Article 6
1. Les États membres prévoient que les données à caractère personnel doivent être:
a) traitées loyalement et licitement;
b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées;
c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;
d) exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;
e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.
2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1.

[2] Article 6
Données relatives au trafic
1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1.

[3] « Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la

A partir de maintenant et en vertu de la nouvelle directive, la rétention de données deviendra une norme et ne sera plus une exception. Les inquiétudes du CCBE concernent (1) la protection du secret professionnel et (2) l'autorisation judiciaire, ainsi que la certitude juridique quant à l'accès aux données.

1/ Secret professionnel

La profession d'avocat s'inquiète des conséquences de la directive qui s'éloigne du principe du respect de la vie privée et de la confidentialité des communications (violation des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne et de l'article 8 de la Convention européenne des droits de l'homme[4]). La directive omet également le droit à la protection des données à caractère personnel (article 8 de la Charte des droits fondamentaux de l'Union européenne). Elle nie le caractère confidentiel de la relation avocat-client et de manière générale le secret professionnel.

Tout le monde a le droit de consulter un avocat pour lui demander des conseils qui peuvent être prodigués si le citoyen est assuré que ses déclarations à l'avocat resteront confidentielles. Ce droit fait partie des droits et libertés fondamentales et découle du principe de l'Etat de droit. Nier ce droit consisterait en une violation grave des droits des défendeurs. L'obligation de secret professionnel d'un avocat sert les intérêts de l'administration judiciaire et en général de l'Etat. Le secret professionnel est un droit pour le client, un devoir de l'avocat. Sans assurance de confidentialité, il ne peut y avoir de confiance et l'avocat ne peut pas jouer son rôle spécifique dans la société.

Dans son arrêt dans l'affaire AM&S[5], la Cour de justice des Communautés européennes mentionne expressément : « *cette confidentialité répond en effet à l'exigence, dont l'importance est reconnue dans l'ensemble des Etats membres, que tout justiciable doit avoir la possibilité de s'adresser en toute liberté à son avocat, dont la profession même comporte la tâche de donner, de façon indépendante, des avis juridiques à tous ceux qui en ont besoin* »[6]. *Elle ajoute que « la protection de la confidentialité de la correspondance entre avocats et clients se fonde principalement sur la reconnaissance de la nature même de la profession d'avocat, en tant qu'elle coopère au maintien de la légalité, dans d'autres Etats membres, cette même protection trouve sa justification dans l'exigence plus spécifique – d'ailleurs reconnue également dans les premiers Etats - du respect des droits de la défense* ». Le devoir de l'avocat de respecter un « *strict secret professionnel* » a été avancé par la Cour dans l'affaire Wouters[7] comme un principe généralement reconnu dans tous les Etats membres et comme « *une règle essentielle pour assurer le bon exercice de la profession d'avocat* » que les barreaux essaient de préserver.

Les informations obtenues par les données de trafic et de localisation sont des questions importantes, d'où l'intérêt d'une telle législation pour les gouvernements. Le fait de pouvoir voir quand, où, comment et combien de fois telle personne consulte un avocat remet sérieusement en cause la confidentialité des relations du client avec son avocat et l'exercice même des droits de la défense. La confidentialité devrait donc bénéficier de la protection de l'Etat et on devrait s'attendre à une protection accrue de la part d'une loi européenne.

---

sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. »

[4] Article 8

1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

[5] Arrêt de la Cour du 18 mai 1982, AM & S Europe Limited contre Commission des Communautés européennes, affaire C-155/79.

[6] Pour une affaire nationale importante, et connue aussi au plan international, voir : Three Rivers District Council and Others v Governor and Company of the Bank of England [2004] UKHL 48.

[7] Arrêt de la Cour du 19 février 2002, Wouters, affaire C-309/99.

2/ la nécessité d'une autorisation judiciaire préalable et une certitude juridique quant à l'accès aux données.

Dans la directive, la rétention est autorisée de manière générale à des fins de recherche, de détection et de poursuite d'*infractions graves* (article 1(1)). Le concept d'infraction grave n'est pas du tout clarifié sur le plan juridique et est ouvert à diverses interprétations.

Dans son avis du 26 septembre 2005 sur le projet de directive, le contrôleur européen de la protection des données (CEPD) souligne le fait qu'une disponibilité suffisante de certaines données relatives au trafic et données de localisation générées peut constituer un instrument précieux pour ces services répressifs et contribuer à la sécurité physique des personnes. Toutefois, le CEPD estime aussi que cela n'implique pas automatiquement la nécessité de nouveaux instruments prévus dans la proposition afférente. Il estime que la nécessité de cette nouvelle obligation de rétention de données – dans sa forme totale - n'a pas encore été démontrée de manière adéquate.

L'article 7 sur la « *protection et sécurité des données* » ne contient aucune mesure de protection importante outre le niveau technique et opérationnel minimum dans l'absolu. Il parle de « *(…) mesures techniques et organisationnelles appropriées afin de garantir que l'accès aux données n'est effectué que par un personnel spécifiquement autorisé* ». En revanche, les Etats membres disposent d'une certaine latitude et aucun paramètre n'est établi malgré ce qui est repris dans le préambule de la directive.

Il n'y a aucune garantie pour les personnes concernées par la rétention de données, mais seulement une référence vague à la directive 95/46/CE et l'opportunité de solutions judiciaires. A nouveau, cela est laissé à la discrétion des Etats membres.

L'article 4 sur « *l'accès aux données* » laisse l'entière responsabilité pour les exigences de nécessité et de proportionnalité à la discrétion des Etats membres. Il semble incorrect d'établir un instrument juridique agressif comme la directive sur la rétention de données au niveau européen sans fixer en même temps des limites ou un niveau adéquat de garantie et de protection juridiques.

Aucune procédure judicaire à respecter n'est prévue pour l'accès aux données, mais seule l'exigence que « *les données conservées ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne (…)dans le respect des exigences de nécessité et de proportionnalité (…), sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme* ». En tout cas, un juge devrait donner l'autorisation d'étendre la période de rétention de données.

Il n'existe aucune disposition relative aux conditions dans lesquelles la rétention est réalisée ou aux autorités de contrôle.

De même, aucune limite de durée des données n'est établie une fois qu'on a pu y accéder et les conserver. L'article 7 (d) établit que toute les données doivent être détruites à la fin de la période de rétention (deux ans selon l'article 6) « *à l'exception des données auxquelles on a pu accéder et qui ont été préservées* ». En revanche, et conformément à l'article 6 de la directive 95/46/CE et à l'article 6, paragraphe 1 de la directive 2002/58/CE, le droit national qui transpose la directive sur la rétention de données devrait veiller à ce que les données transmises par un opérateur au gouvernement ou à l'autorité répressive, dans le cadre de la procédure judiciaire à cet effet, soient conservées aussi longtemps que nécessaire pour l'objectif pour lequel les données avaient été transmises à l'origine. Les données ne peuvent pas être utilisées par le gouvernement ou l'autorité répressive à tout autre fin que celle qui a été avancée à l'origine.

Selon l'article 11, les conditions établies à l'article 15 de la directive 2002/58/CE, contenant les dispositions de l'article 8(2) de la Convention européenne des droits de l'homme, sont exclues de manière explicite lors de l'application aux données réglementées par la directive sur la rétention de données. Le texte de l'article 11 n'est pas assez explicite sur le fait que les Etats membres ne sont plus compétents pour l'adoption d'une législation relative aux infractions pénales outre la proposition

actuelle. Cela crée une ambiguïté sur les compétences restantes des Etats membres pour adopter une législation relative à la rétention de données.

Pour ces raisons, le CCBE croit fermement que l'accès aux données devrait faire l'objet d'une autorisation judiciaire préalable dans tous les cas de figure.